UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

IN RE LASTPASS DATA SECURITY INCIDENT LITIGATION	)	Civil Action No. 22-12047

MEMORANDUM AND ORDER

July 30, 2024

Saris, D.J.

INTRODUCTION

LastPass sells encrypted digital "vaults" in which customers can store personal information. LastPass claims no one other than the customer -- not even LastPass -- has access to a vault's decrypted contents. In August 2022, a third party hacked into a LastPass employee's home computer, accessed LastPass's development environment, and acquired a copy of customers' encrypted vault files. The hacker also exfiltrated customers' account information and metadata, which were not encrypted. Plaintiffs are LastPass customers whose data was compromised during the data breach. They bring this putative class action against LastPass and its former parent company, GoTo Technologies USA, Inc., alleging twenty-two causes of action.[1] Defendants move to dismiss all counts under Rule

[1] Plaintiffs bring eight claims on behalf of a nationwide class against both Defendants: negligence (Count I); negligent misrepresentation (Count II); breach of contract (Count III);

12(b)(1) for lack of standing, and under Rule 12(b)(6) for failure to state a claim. After a hearing, the Court **ALLOWS IN PART** and **DENIES IN PART** Defendants' motion (Dkt. 92).

---

breach of implied contract (Count IV); breach of fiduciary duty (Count V); breach of the covenant of good faith and fair dealing (Count VI); unjust enrichment (Count VII); and declaratory and injunctive relief (Count VIII). They bring claims under the Massachusetts Consumer Protection Act, Mass. Gen. Laws ch. 93A, §§ 1, et seq., against both Defendants on behalf of a nationwide class and a Massachusetts subclass (Counts IX & X). On behalf of state-specific subclasses, Plaintiffs allege LastPass violated the Arizona Consumer Fraud Act, Ariz. Rev. Stat. §§ 44-1521, et seq. (Count XI); the California Unfair Competition Law, Cal. Bus. & Prof. Code §§ 17200, et seq. (Count XII); the California Consumer Legal Remedies Act, Cal. Civ. Code §§ 1750, et seq. (Count XIII); the California Customer Records Act, Cal. Civ. Code §§ 1798.80, et seq. (Count XIV); the California Consumer Privacy Act, Cal. Civ. Code §§ 1798.100, et seq. (Count XV); the Florida Deceptive and Unfair Trade Practices Act, Fla. Stat. §§ 501.201, et seq. (Count XVI); the Illinois Personal Information Protection Act, 815 Ill. Comp. Stat. §§ 530/10(a), et seq. (Count XVII); the Illinois Consumer Fraud and Deceptive Business Practices Act, 815 Ill. Comp. Stat. §§ 505, et seq. (Count XVIII); the Illinois Deceptive Trade Practices Act, 815 Ill. Comp. Stat. §§ 510/1, et seq. (Count XIX); the New York General Business Law, N.Y. Gen. Bus. Law §§ 349, et seq. (Count XX); the Oklahoma Consumer Protection Act, Okla. Stat. tit. 15, §§ 751, et seq. (Count XXI); and the Pennsylvania Unfair Trade Practices and Consumer Protection Law, 73 Pa. Cons. Stat. §§ 201-1, et seq. (Count XXII).

BACKGROUND

Drawing all inferences in favor of Plaintiffs, the facts as alleged in the consolidated class action complaint are as follows.[2]

I. The Product

Defendant LastPass US LP is a limited partnership incorporated in Delaware and principally doing business in Massachusetts. It provides online password management services to over "33 million users and 100,000 businesses worldwide." Dkt. 86 at 1. Defendant GoTo Technologies USA, Inc. ("GoTo"), formerly known as "LogMeIn," acquired LastPass in 2015. GoTo provides "software and cloud-based remote work tools." Dkt. 86 at 40.

LastPass offers paid subscription-based accounts for individual consumers, families, and businesses. It also offers free individual consumer accounts with limited features. LastPass's primary product is a password manager "vault" in which users can store login credentials to websites and personal information like credit card, Social Security, financial account, and driver's license numbers. This information is then encrypted and accessible to the customer via a single "master password," a

[2] The consolidated complaint relies on statements Defendants made on their websites. The pages cited are merged into the consolidated complaint. See Alt. Energy, Inc. v. St. Paul Fire & Marine Ins. Co., 267 F.3d 30, 33 (1st Cir. 2001) ("When the complaint relies upon a document, whose authenticity is not challenged, [it] 'merges into the pleadings' and the court may properly consider it under a Rule 12(b)(6) motion to dismiss.").

password created solely to access the vault. The vault also contains unencrypted data including URLs to the websites corresponding to passwords within the vault and "certain use cases involving email addresses." See Dkt. 86 at 61-62; Dkt. 92-1 at 18.

LastPass does not store or otherwise know users' master passwords. However, LastPass retains unencrypted customer account information and metadata, including "company names, end-user names, billing addresses, email addresses, telephone numbers, [and] IP addresses from which customers were accessing the LastPass service." Dkt. 86 at 54.

II. The Breach

In August 2022, a hacker targeted a LastPass employee's home computer through a third-party application and used a keylogging software to obtain the employee's internal account credentials. The hacker used those credentials to log into LastPass's online development environment. There, the hacker exfiltrated encrypted vault backups and unencrypted user information including names, billing addresses, email addresses, IP addresses, and related metadata. Plaintiffs Amy Doermann, Ayana Looney, Dan LeFebvre, David Andrew, Erik Brook, Glenn Mulvenna, Hui Li, Joel Eagelston, Josh Shi, Nathan Goldstein, Noah Bunag, R. Andre Klein, Sarb Dhesi, and Steven Carter are individual LastPass users whose data was

compromised by the breach.[3] Mulvenna, Li, and Bunag used free accounts. Doermann's employer paid for her account. The others paid for their LastPass subscriptions. Plaintiffs Hustle N Flow Ventures, LLC ("Hustle N Flow") and Debt Cleanse Group Legal Services LLC ("Debt Cleanse") are companies that purchased business subscriptions from LastPass.[4] Personal information belonging to their employees, clients, and contractors was compromised during the breach.

III. Notification

On August 25, 2022, LastPass issued its first notice to Plaintiffs informing them of the data breach. In this notice, LastPass asserted that there was "no evidence of any unauthorized access to encrypted vault data" and that users' master passwords remained uncompromised. Dkt. 95-1 at 8. LastPass stated in this notice that it had begun an investigation into the data breach. Then, on September 15, 2022, LastPass issued a second notice to Plaintiffs informing them that it had concluded its investigation. LastPass again stated that there was "no evidence that this

[3] Doermann, Klein, and Carter are residents of New York. Looney, Bunag, and Dhesi are residents of California. Andrew, Brook, Li, and Shi are residents of Illinois, but Brook resided in California and Li resided in Pennsylvania when they signed up for LastPass. LeFebvre, Mulvenna, Eagelston, and Goldstein are residents of Oklahoma, Florida, Arizona, and Massachusetts, respectively.

[4] Hustle N Flow is a limited liability company organized and headquartered in Florida. Debt Cleanse is a Delaware limited liability company with its primary place of business in Illinois.

incident involved any access to customer data or encrypted password vaults," but noted that the hacker had "persistent access" to the development environment over a period of four days in August 2022. Dkt. 95-1 at 6-7.

On November 30, 2022, LastPass provided a third notice, this time informing users that, using information obtained in the August 2022 data breach, LastPass believed a threat actor had been able to obtain additional information through a third-party cloud storage service. LastPass continued to assert that users' vault data remained encrypted. On December 22, 2022, LastPass provided a fourth update. In this notice, LastPass revealed that the threat actor had been able to obtain a copy of "a backup of customer vault data," which was encrypted but could be decrypted if the threat actor were able to use "brute force" to guess a user's master password. Dkt. 95-1 at 4.[5] In response, LastPass stated that it was implementing additional security measures to prevent additional data breaches.

On March 1, 2023, LastPass provided users with a final update on the data breach. In this notice, Last Pass confirmed the threat actor had been able to access users' encrypted and unencrypted vault data. This update also suggested ways for users to strengthen

[5] "Brute force attacks are when a bad actor deploys multiple means and attempts to guess or decipher account login credentials (usernames and passwords)." Dkt. 110 at 4-5.

their data security to prevent theft of their data in the event of a future breach.

IV. Harm

Plaintiffs allege malicious third-party actors used "brute force" to guess some of their master passwords and decrypt their vault data. See Dkt. 86 at 62. This has led to "the exposure, misappropriation, and misuse of millions of users' information through fraud, identity theft, phishing scams, credit-stuffing attacks, and various other kinds of injury." Id. at 2. Some injuries are common to the class. Others are specific to certain groups of plaintiffs.

Plaintiffs all have spent time responding to the breach that they would otherwise have used on "other activities, such as work or recreation." See, e.g., id. at 5, 39-40 (Debt Cleanse and Hustle N Flow noting their employees would have spent time on other activities). Plaintiffs believe they will need to continue devoting time responding to the breach in the future. And all Plaintiffs except for Debt Cleanse allege a "substantially increased risk of fraud, identity theft, and misuse" in the future, as well as garden variety emotional distress. See, e.g., id. at 6.

Plaintiffs who paid for subscriptions -- all Plaintiffs except for Doermann, Mulvenna, Li, and Bunag, who got free subscriptions -- claim they did not receive "the level of security that Defendants touted throughout their marketing materials." See,

e.g., id. at 8. They claim they would not have paid as much as they did for LastPass's service had they known of its flaws. Moreover, Plaintiffs except for Debt Cleanse, Hustle N Flow, and Dhesi allege "damages to and diminution in the value" of their sensitive personal information, which they contend is "a form of intangible property." See, e.g., Dkt. 86 at 6.

Nine of the sixteen Plaintiffs -- Doermann, LeFebvre, Brook, Mulvenna, Li, Shi, Bunag, Dhesi, and Carter -- allege they have suffered actual or attempted fraud, including theft from online wallets, attempted unauthorized credit card charges, or unauthorized applications for loans and credit cards. Two Plaintiffs -- Bunag and Carter -- allege they have received alerts from credit monitoring agencies that their data is being sold on the "dark web." And six Plaintiffs -- Doermann, Looney, Shi, Goldstein, Bunag, and Carter -- report increased phishing attempts and spam messages.

Eight Plaintiffs -- Doermann, LeFebvre, Andrew, Mulvenna, Bunag, Dhesi, Carter, and Hustle N Flow -- have spent money responding to the breach. Mitigation costs have included payments to mental health providers, fees for replacement password management software, subscriptions for identity-theft-protection and credit-monitoring services, and fees associated with canceling and replacing accounts.

DISCUSSION

"When faced with motions to dismiss under both 12(b)(1) and 12(b)(6), a district court, absent good reason to do otherwise, should ordinarily decide the 12(b)(1) motion first." Ne. Erectors Ass'n of BTEA v. Sec'y of Lab., 62 F.3d 37, 39 (1st Cir. 1995).

I. Motion to Dismiss for Lack of Standing

Defendants move to dismiss the complaint under Federal Rule of Civil Procedure 12(b)(1), asserting Plaintiffs do not have standing to sue. The Court accepts Plaintiffs' well-pleaded factual allegations and "draw[s] all reasonable inferences in [their] favor." See Merlonghi v. United States, 620 F.3d 50, 54 (1st Cir. 2010).

A. Legal Standard

Pursuant to Rule 12(b)(1), a party may move to dismiss for a lack of subject-matter jurisdiction. See Fed. R. Civ. P. 12(b)(1). Standing to sue is one of the requirements of subject-matter jurisdiction, so the lack of standing is a basis for dismissal under Rule 12(b)(1). "To establish Article III standing, a plaintiff must show (1) an injury in fact, (2) a sufficient causal connection between the injury and the conduct complained of, and (3) a likelihood that the injury will be redressed by a favorable decision."[6] Susan B. Anthony List v. Driehaus, 573 U.S. 149, 157-58

[6] This consolidated class action involves eight cases filed in federal court and one case Defendants removed from state court.

(2014) (cleaned up) (quoting Lujan v. Defs. of Wildlife, 504 U.S. 555, 560-61 (1992)). An "injury in fact" must be "both concrete and particularized" and "actual or imminent, not conjectural or hypothetical." Spokeo, Inc. v. Robins, 578 U.S. 330, 339 (2016) (quoting Lujan, 504 U.S. at 560).

B. Discussion

Defendants contend Plaintiffs have not alleged a sufficient "injury in fact" to support standing. Alternatively, they argue that they did not cause any cognizable "injury in fact" the Plaintiffs suffered.

1. Injury in Fact

Among other injuries, Plaintiffs all claim to have spent time responding to the breach that they would otherwise have dedicated to work or recreation. "[T]ime spent responding to a data breach can constitute a concrete injury sufficient to confer standing" where the "time would otherwise have been put to profitable use" and it was spent in "response to a substantial and imminent risk of harm." Webb v. Injured Workers Pharmacy, LLC, 72 F.4th 365, 377 (1st. Cir. 2023) (citing Clapper v. Amnesty Int'l USA, 568 U.S. 398, 422 (2013)). Defendants assert that "encrypted sensitive data

---

Plaintiffs argue that because Defendants invoked federal jurisdiction in one of the nine consolidated cases, they have "conceded Article III subject matter jurisdiction." Dkt. 103 at 22. But the Court has "an obligation to inquire into [its] subject matter jurisdiction" in every case. See One & Ken Valley Hous. Grp. v. Me. State Hous. Auth., 716 F.3d 218, 224 (1st Cir. 2013).

stored in [Plaintiffs'] vaults was not impacted" by the data breach, so any risk of harm was "pure[ly] speculat[ive]" rather than "imminent." See Dkt. 95 at 25.

Plaintiffs have plausibly shown injury in fact. In Webb, the First Circuit outlined three factors that inform whether the risk of misuse after a data breach is "imminent and substantial" for the purposes of standing. See Webb, 72 F.4th at 375. First, courts consider whether the "information [wa]s deliberately taken by thieves intending to use the information to their financial advantage -- i.e., exposed in a targeted attack rather than inadvertently." Id. Second, courts look to whether "at least some information stolen in [the] data breach has already been misused." Id. at 376. And third, courts evaluate whether "the compromised data is particularly sensitive." Id.

Allegations in the consolidated complaint meet the mark. First, parties agree the data breach resulted from a deliberate attack on LastPass's development environment. Second, Plaintiffs plausibly allege actual and attempted misuse of their compromised data, including theft from online wallets, fraudulent credit card charges, unauthorized applications for loans and credit cards, sale of information on the "dark web," and increased phishing attempts and spam messages. Finally, at least some stolen data was highly sensitive. Vaults contained Plaintiffs' Social Security numbers, driver's license numbers, and login credentials to

banking and financial accounts. The vaults also housed unencrypted copies of Plaintiffs' names, billing addresses, email addresses, and other metadata. Plaintiffs have plausibly shown they face a real and imminent threat of misuse of their data, so their lost time constitutes injury in fact.

2. Causation

Plaintiffs also contend Defendants caused their injuries. Injuries are "fairly traceable" to a defendant's conduct for the purposes of Article III standing if plaintiffs plausibly allege the defendant's "actions led to the exposure and actual or potential misuse of the plaintiffs'" personal information. See Webb, 72 F.4th at 377 (citing In re Evenflo Co., Mktg., Sales Pracs. & Prods. Liab. Litig., 54 F.4th 28, 41 (1st Cir. 2022)). Defendants counter that the breach could not plausibly have caused Plaintiffs' injuries because "the only data compromised" by the breach was "non-sensitive," and sensitive vault data "remains encrypted and unreadable." Dkt. 92-1 at 22.

Plaintiffs meet the requirements of Article III causation. Plaintiffs claim Defendants' lack of internal cybersecurity protocols enabled a hacker to obtain an employee's credentials, access LastPass's internal development environment, and exfiltrate both encrypted vault files and unencrypted account information and metadata. They also allege Defendants' substandard password-encryption algorithms allowed bad actors then to easily use "brute

force" to decrypt Plaintiffs' vaults. Finally, Plaintiffs assert Defendants delayed notifying them of the breach's full scope, stymying Plaintiffs' ability to mitigate the data breach's harm effectively and increasing their exposure. Plaintiffs have shown an "obvious temporal connection" between the data breach and actual misuse of some of their data. See Webb, 72 F.4th at 374. Moreover, they have plausibly alleged third parties obtained their sensitive information from the data breach and not from elsewhere. Id. (noting plaintiff was "very careful" with sensitive information and stored it only in secure locations, leading to the "obvious inference" that those who had misused sensitive information obtained it from the breach, not another source); see, e.g., Dkt. 86-1 at 40-41 (alleging Plaintiffs who suffered theft lost only from those accounts with credentials saved in their vaults, and not from other accounts). The cases Defendants cite are inapposite. See, e.g., Katz v. Pershing, LLC, 672 F.3d 64, 79-80 (1st Cir. 2012) (no standing because plaintiffs did not allege actual misuse); Hartigan v. Macy's, Inc., 501 F. Supp. 3d 1, 5 (D. Mass. 2020) (same, and because "information stolen was not highly sensitive or immutable"); Baysal v. Midvale Indem. Co., 78 F.4th 976, 977-78 (7th Cir. 2023) (no standing because alleged harm -- unauthorized brokerage transaction -- was not plausibly related to

exposure of plaintiffs' driver's license numbers). As a result, the Court **DENIES** the motion to dismiss for lack of standing.[7]

II. Motion to Dismiss for Failure to State a Claim

A. Legal Standard

To survive a motion to dismiss, a complaint must allege "a plausible entitlement to relief." Bell Atl. Corp. v. Twombly, 550 U.S. 544, 559 (2007). "While a complaint attacked by a Rule 12(b)(6) motion does not need detailed factual allegations, a plaintiff's obligation to provide the grounds of his entitlement to relief requires more than labels and conclusions, and a formulaic recitation of a cause of action's elements will not do." Id. at 555 (cleaned up). That standard requires the Court to "separate the complaint's factual allegations (which must be accepted as true) from its conclusory legal allegations (which need not be credited)." Kando v. R.I. State Bd. of Elections, 880 F.3d 53, 58 (1st Cir. 2018) (quoting Morales-Cruz v. Univ. of P.R., 676 F.3d 220, 224 (1st Cir. 2012)). The Court must then determine whether the factual allegations permit it "to draw the reasonable

[7] The Court need not address whether Plaintiffs' other injuries suffice for Article III standing. See Webb, 72 F.4th at 377–78 (declining to rule on additional alleged injuries because the Court had identified "at least one injury in fact caused by the defendant and redressable by a court order"); accord Attias v. Carefirst, Inc., 865 F.3d 620, 626 n.2 (D.C. Cir. 2017) (noting in data breach suit that the court "need not address" other injuries, including actual misuse, because plaintiffs had standing "based on their heightened risk of future identity theft").

inference that the defendant is liable for the misconduct alleged." Germanowski v. Harris, 854 F.3d 68, 72 (1st Cir. 2017) (quoting Ashcroft v. Iqbal, 556 U.S. 662, 678 (2009)).

B. Discussion

1. Claims Against GoTo

Plaintiffs raise ten claims against GoTo: negligence (Count I), negligent misrepresentation (Count II), breach of contract (Count III), breach of implied contract (Count IV), breach of fiduciary duty (Count V), breach of the covenant of good faith and fair dealing (Count VI), unjust enrichment (Count VII), declaratory and injunctive relief (Count VIII), and violations of the Massachusetts Consumer Protection Act ("Chapter 93A") (Counts IX & X). Plaintiffs allege GoTo is LastPass's parent company and "influences and controls" its activity. Dkt. 86 at 43. GoTo allegedly suffered data breaches in the past and knew about LastPass's vulnerabilities when it acquired LastPass. GoTo and LastPass allegedly shared cloud storage at the time of the data breach. Finally, GoTo's "terms of service" allegedly state it "maintain[s] a global privacy and security program," is "dedicated to monitoring and continuously improving [its] security, technical and organizational measures," that it is "always evaluating industry standard practices regarding technical data privacy and information security," and that it "strive[s] to meet or exceed those standards." Dkt. 86 at 96-97.

No Plaintiff claims to have transacted with GoTo, read its "terms of service," or relied on any of GoTo's representations. Plaintiffs do not plausibly allege GoTo caused them injury directly. Neither the consolidated complaint nor Plaintiffs' brief argues GoTo should be vicariously liable for LastPass's conduct. As a result, the motion to dismiss is **ALLOWED** as to all claims against GoTo.

2. Cognizable Injury

Plaintiffs must allege actual injury or loss as an element of many of their common law claims. For example, under Massachusetts law,[8] damages are an element of claims of negligence, negligent misrepresentation, breach of contract, breach of implied contract, breach of fiduciary duty, and breach of the covenant of good faith and fair dealing.[9] Loss or injury is also an element of many of Plaintiffs' state statutory claims. LastPass argues Plaintiffs do not "plausibly plead a cognizable loss" because their "general allegations of lost time, continued risk to [their] personal data, and the danger of future harm are not cognizable injuries." See

[8] For now, LastPass frames its argument primarily in terms of Massachusetts law.

[9] See Donovan v. Philip Morris USA, Inc., 914 N.E.2d 891, 899 (Mass. 2009) (negligence); Nota Constr. Corp. v. Keyes Assocs., Inc., 694 N.E.2d 401, 405 (Mass. App. Ct. 1998) (negligent misrepresentation) Hanover Ins. Co. v. Sutton, 705 N.E.2d 279, 288-89 (Mass. App. Ct. 1999) (fiduciary duty); Singarella v. City of Bos., 173 N.E.2d 290, 291 (Mass. 1961) (contract); Grant v. Target Corp., 126 F. Supp. 3d 183, 190 (D. Mass. 2015) (covenant of good faith and fair dealing).

Dkt. 92-1 at 28-29 (cleaned up) (quoting Griffey v. Magellan Health Inc., 562 F. Supp. 3d 34, 44-45 (D. Ariz. 2021)). LastPass's arguments fall short.

First, as to Massachusetts law, at least eight Plaintiffs -- LeFebvre, Brook, Mulvenna, Li, Shi, Bunag, Dhesi, and Carter -- allegedly suffered actual pecuniary loss due to the breach. Three others -- Doermann, Andrew, and Debt Cleanse -- apparently spent money mitigating the effects of the breach. These are cognizable injuries. See Weekes v. Cohen Cleary P.C., No. 23-10817, 2024 WL 1159642, at *4 (D. Mass. Mar. 15, 2024) (holding that "damages caused by the actual misuse or efforts expended to prevent imminent misuse of" exposed data "satisfy the damages requirement"). The remaining Plaintiffs plead that due to the substantial risk their data will be misused, they will need to continue monitoring their accounts in the future. Costs of future credit monitoring are also cognizable injuries. In re Shields Health Care Grp., Inc. Data Breach Litig., No. 22-10901, 2024 WL 939219, at *6 (D. Mass. Mar. 5, 2024) ("Where Plaintiffs show a substantial risk of harm manifesting in the future, the 'element of injury and damage will have been satisfied and the cost of that monitoring is recoverable in tort.'" (quoting Donovan v. Philip Morris USA, Inc., 914 N.E.2d 891, 901 (Mass. 2009))).

LastPass's arguments fare no better as to Plaintiffs' statutory causes of action. LastPass cites no authority indicating

the injuries alleged are not cognizable under state consumer protection statutes. See, e.g., Nightingale v. Nat'l Grid USA Serv. Co., No. 23-1476, 2024 WL 3337766, at *6 (1st Cir. July 9, 2024) (holding "excessive debt collection calls" are cognizable injuries under Chapter 93A). Thus, the Court declines to dismiss Plaintiffs' claims for failure to plead a cognizable injury.

3. Negligence (Count I)

Plaintiffs allege LastPass negligently "fail[ed] to provide fair, reasonable, or adequate computer systems and data security practices to safeguard the PII and financial information of Plaintiffs and Class Members." Dkt. 86 at 87. Additionally, Plaintiffs plead negligence per se based on LastPass's alleged violations of the Federal Trade Commission Act, 15 U.S.C. § 45 ("FTC Act"), and other laws. To state a claim for negligence, Plaintiffs must show "(1) a legal duty owed to the[m] by the defendant[s]; (2) a breach of that duty by the defendant[s]; (3) causation; and (4) actual loss by the plaintiff[s]." See Delaney v. Reynolds, 825 N.E.2d 554, 556 (Mass. App. Ct. 2005) (citing Glidden v. Maglio, 722 N.E.2d 971, 973 (Mass. 2000)). LastPass argues Plaintiffs have not demonstrated proximate cause, and alternatively, that the economic loss doctrine precludes Plaintiffs' recovery in tort. The Court addresses the economic loss doctrine first.

The economic loss doctrine prohibits recovery in tort "unless

the plaintiffs can establish that the injuries they suffered due to the [defendant's] negligence involved physical harm or property damage, and not solely economic loss." Cumis Ins. Soc'y, Inc. v. BJ's Wholesale Club, Inc., 918 N.E.2d 36, 46-47 (Mass. 2009) (holding in data breach case that "costs of replacing credit cards for compromised accounts[] were economic losses" barred by the doctrine); see In re TJX Cos. Retail Sec. Breach Litig., 564 F.3d 489, 498-99 (1st Cir. 2009). The economic loss doctrine does not apply to negligence claims against a fiduciary. See Szulik v. State St. Bank & Tr. Co., 935 F. Supp. 2d 240, 271 n.11 (D. Mass. 2013); see also Portier v. NEO Tech. Sols., No. 17-30111, 2019 WL 7946103, at *21 (D. Mass. Dec. 31, 2019) (recommending economic loss doctrine not apply because of "special relationship" between plaintiff and defendant), report and recommendation adopted, 2020 WL 877035 (D. Mass. Jan. 30, 2020). Plaintiffs allege economic injuries. Thus, unless an exception applies, the economic loss doctrine bars their negligence claim.

Plaintiffs counter that the duties at issue are independently "imposed by several state and federal laws" such the FTC Act and the Massachusetts Data Security statute ("Chapter 93H"). See Mass. Gen. Laws ch. 93H, § 2; 201 Mass. Code Regs. 17.01-.05.[10] But these

[10] The FTC Act prohibits "[u]nfair methods of competition" and "unfair or deceptive acts or practices" involving commerce. See 15 U.S.C. § 45(a)(1). Chapter 93H and its regulations impose a duty on "[e]very person that owns or licenses personal information about

statutes do not establish a duty cognizable in negligence. See Juliano v. Simpson, 962 N.E.2d 175, 179 (Mass. 2012) ("The Commonwealth does not follow the doctrine of negligence per se, whereby . . . violation of a statute, without more, may establish a breach of duty."); accord Eggiman v. Bank of Am., N.A., No. 22-10298, 2023 WL 2647071, at *4 (D. Mass. Mar. 27, 2023) (same). Plaintiffs also have not shown a special or fiduciary relationship exists that would give rise to negligence claims not barred by the economic loss doctrine.[11] Thus, LastPass's motion to dismiss is **ALLOWED** as to Plaintiffs' negligence and negligence per se claims (Count I).

4. Negligent Misrepresentation (Count II)

Plaintiffs claim LastPass negligently misrepresented the quality of its data security. To state a claim for negligent misrepresentation, a plaintiff must show the defendant "(1) made a false representation of material fact; (2) with knowledge of its falsity; (3) for the purpose of inducing the plaintiff to act on this representation; (4) that the plaintiff reasonably relied on the representation as true; and (5) that the plaintiff acted upon it to their damage." AcBel Polytech, Inc. v. Fairchild Semiconductor Int'l, Inc., 928 F.3d 110, 122 (1st Cir. 2019)

a resident" to "maintain a comprehensive information security program." 201 Mass. Code Regs. 17.03.

[11] The Court discusses Plaintiffs' fiduciary duty claim below.

(cleaned up). LastPass responds that Federal Rule of Civil Procedure 9(b)'s heightened pleading standard applies, and Plaintiffs fail to meet it. Alternatively, LastPass argues the merger clause in its "terms of service" precludes recovery for negligent misrepresentation.

Negligent misrepresentation claims are subject to Rule 9(b) "where the core allegations effectively charge fraud." See N. Am. Cath. Educ. Programming Found., Inc. v. Cardinale, 567 F.3d 8, 15 (1st Cir. 2009). Here, Plaintiffs do not appear to do so. Regardless of whether Rule 9(b) applies, Plaintiffs have alleged enough to state a plausible claim. LastPass promises in its "terms of service" for business customers that it agrees to "comply with all applicable laws, rules and regulations including . . . privacy [and] data protection laws," and to "maintain appropriate organizational, administrative, and technical safeguards . . . in accordance with industry standards." See Dkt. 92-5 at 7-8. Plaintiffs allege LastPass required only "100,100 iterations of the PBKDF2 algorithm to secure customers' master passwords, which is well below the [industry] standard 310,000 iterations." See Dkt. 86 at 53. Debt Cleanse says it read these terms in 2015 and relied on them when deciding to pay for LastPass's services.

LastPass's merger clause does not shield it from Debt Cleanse's claim. LastPass's "terms of service" contain a provision stating that the terms "set[] forth the entire agreement . . . and

supersede[] all prior and contemporaneous oral and written agreements." See Dkt. 92-5 at 12. Although merger clauses generally are "enforced against . . . negligent misrepresentation claim[s]," see Amorim Holding Financeria, S.G.P.S., S.A. v. C.P. Baker & Co., 53 F. Supp. 3d 279, 302-03 (D. Mass. 2014), Debt Cleanse alleges LastPass's "terms of service" contained false statements. Thus, the merger clause does not apply as to Debt Cleanse.

Other than Debt Cleanse, most Plaintiffs have not alleged "false representation[s] of material fact" on which they relied. Hustle N Flow claims "one of [LastPass]'s marketing or sales agents" made verbal promises over the phone about data security, see Dkt. 86 at 39, but the merger clause in LastPass's "terms of service" precludes a negligent misrepresentation claim based on those promises, Amorim, 53 F. Supp. 3d at 302-03.

As a result, the motion to dismiss is **DENIED** as to Debt Cleanse's negligent misrepresentation claim against LastPass but is otherwise **ALLOWED** (Count II).

5. Breach of Contract (Count III)

Plaintiffs with paid accounts[12] allege LastPass breached its "terms of service" by not maintaining "appropriate organizational,

[12] The consolidated complaint lists the name of every Plaintiff except Doermann for this count. See Dkt 86 at 95. Directly under the names, the consolidated complaint states that "Plaintiffs bring this claim . . . on behalf of individuals and entities that paid for LastPass accounts." Id.

administrative, and technical safeguards." Dkt. 86 at 50. To state a claim for breach of contract, Plaintiffs must allege that: "(1) a valid contract between the parties existed, (2) the plaintiff was ready, willing, and able to perform, (3) the defendant was in breach of the contract, and (4) the plaintiff sustained damages as a result." Omori v. Brandeis Univ., 635 F. Supp. 3d 47, 52 (D. Mass. 2022) (quoting In re Bos. Univ. COVID-19 Refund Litig., 511 F. Supp. 3d 20, 23 (D. Mass. 2021)). LastPass does not deny the existence of a contract but argues Plaintiffs have not plausibly alleged breach. Alternatively, LastPass states its "terms of service" contain a limitation-of-liability provision that "precludes Plaintiffs' consequential damages." Dkt. 92-1 at 36.

a. Breach

Parties agree LastPass's "terms of service" required it to "implement[] and maintain appropriate organizational, administrative, and technical safeguards designed to protect [Plaintiffs'] [c]ontent against any unauthorized access, loss, misuse, or disclosure." See Dkt. 92-1 at 34 (quoting Dkt. 92-5 at 7). Plaintiffs allege LastPass did not provide "appropriate" safeguards, for example, by requiring only "100,100 iterations of the PBKDF2 algorithm to secure customers' master passwords, which is well below the [industry] standard 310,000 iterations." See Dkt. 86 at 53. Plaintiffs claim LastPass also did not "update its master password encryption requirements since as early as 2018."

Id. Finally, Plaintiffs contend LastPass "[f]ail[ed] to maintain adequate and appropriate oversight and audits on [its] internal data security and [its] employees, vendors, [and] contactors." Id. at 97. That is enough to plausibly plead LastPass failed to provide "appropriate" cybersecurity protocols.

b. Limitation of Liability

Next, LastPass asserts that the limitation of liability provision in its "terms of service" precludes liability for consequential damages. Plaintiffs respond that the provision is unconscionable, or alternatively, that they seek only direct damages, which are not precluded.

To prove a term is unconscionable, "a plaintiff must show both substantive unconscionability (that the term[] [is] oppressive to one party) and procedural unconscionability (that the . . . aggrieved party had no meaningful choice and was subject to unfair surprise)." Machado v. System4 LLC, 28 N.E.3d 401, 414 (Mass. 2015) (cleaned up). Plaintiffs make neither showing here.

So, the Court turns to the nature of the damages. LastPass's "terms of service" include a provision disclaiming liability "for any indirect, special, consequential, incidental, exemplary, or other such damages or losses." See Dkt. 92-5 at 9; Dkt. 92-6 at 8. So-called "direct damages" are "the natural and probable consequences of the breach, that is, those arising naturally according to the usual course of things, from such breach of

contract itself." See Boylston Hous. Corp. v. O'Toole, 74 N.E.2d 288, 302 (Mass. 1947) (internal quotation marks omitted). By way of contrast, "[c]onsequential damages are damages that do not arise naturally or ordinarily from a breach of contract, but which arise because of the intervention of special circumstances." Chestnut Hill Dev. Corp. v. Otis Elevator Co., 739 F. Supp. 692, 701 (D. Mass. 1990) (citing Boylston, 74 N.E.2d at 302). The question is whether Plaintiffs' damages are direct or consequential.

Courts generally treat lost benefits of the bargain as direct damages. See Atlantech Inc. v. Am. Panel Corp., 743 F.3d 287, 293 (1st Cir. 2014); see also Restatement (Second) of Contracts § 347 cmt. a (Am. L. Inst. 1981) (noting that damages in contract "are ordinarily based on the injured party's expectation interest and are intended to give him the benefit of his bargain"). Plaintiffs transacted with LastPass specifically for the provision of data security. They allege LastPass knew customers placed sensitive information in their vaults and failed to provide adequate security as promised. Costs to mitigate the misuse of customers' data flow directly and foreseeably from that breach of contract. Cf. Restatement (Second) of Contracts § 351 cmt. a (Am. L. Inst. 1981) ("A contracting party is generally expected to take account of those risks that are foreseeable at the time he makes the contract."). The case LastPass cites is easily distinguishable and does not pass muster. See In re Brinker Data Incident Litig., No.

18-686, 2020 WL 691848, at *13 (M.D. Fla. Jan. 27, 2020) (holding that "unauthorized charges, lost time, and lost cash-back rewards [we]re all consequential damages" because the "subject of the consumer transaction" was "the food or drinks that Plaintiffs purchased" from the defendant restaurant company, not data security). LastPass's motion to dismiss is **DENIED** as to Plaintiffs' breach of contract claim (Count III).

6. Breach of Implied Contract (Count IV)

"In the absence of an express agreement, an implied contract may be inferred" from "the conduct" and "relationship of the parties." See T.F. v. B.L., 813 N.E.2d 1244, 1249 (Mass. 2004). "A contract implied in fact requires the same elements as an express contract and differs only in the method of expressing mutual assent." Mass. Eye & Ear Infirmary v. QLT Phototherapeutics, Inc., 412 F.3d 215, 230 (1st Cir. 2005) (citation omitted). Alternatively, a court may find a contract implied in law "for reasons of justice" where "reasonable expectations" of the plaintiffs "are defeated." See Salamon v. Terra, 477 N.E.2d 1029, 1031 (Mass. 1985) (cleaned up) (quoting 1 A. Corbin, Contracts § 19 (1963)); Liss v. Studeny, 879 N.E.2d 676, 682-83 (Mass. 2008).

Plaintiffs allege LastPass violated implied contractual duties to safeguard their data. All Plaintiffs (paying and nonpaying) agreed to the "terms of service," which require LastPass to provide "appropriate" safeguards for Plaintiffs' sensitive

information. LastPass does not dispute that it is bound by those terms. See Dkt. 92-1 at 36-37. The motion to dismiss is **ALLOWED** as to Plaintiffs' breach of implied contract claim (Count IV).

7. Breach of Fiduciary Duty (Count V)

Plaintiffs allege LastPass breached a fiduciary duty to maintain their personal information securely by failing to prevent the data breach. To state a claim for breach of fiduciary duty, Plaintiffs must show "(1) the existence of a duty of a fiduciary nature, based upon the relationship of the parties, (2) breach of that duty, and (3) a causal relationship between that breach and some resulting harm to the plaintiff." In re Shields, 2024 WL 939219, at *6 (quoting Amorim, 53 F. Supp. 3d at 295). LastPass counters that no fiduciary relationship existed here.

Fiduciary relationships are defined by one party's "trust and confidence . . . in the integrity and fidelity of another." See Est. of Moulton v. Puopolo, 5 N.E.3d 908, 921 (Mass. 2014). They may arise either "as a matter of law, where parties to the subject relationship are cast in [certain] archetypal roles," or "as determined by the facts established upon evidence indicating that one person is in fact dependent on another's judgment in business affairs or property matters." UBS Fin. Servs., Inc. v. Aliberti, 133 N.E.3d 277, 288 (Mass. 2019) (cleaned up) (citations omitted). Fiduciary relationships normally do not arise from "business transactions conducted at arm's length," but may where "one party

reposes its confidence in another." Indus. Gen. Corp. v. Sequoia Pac. Sys. Corp., 44 F.3d 40, 44 (1st Cir. 1995).

Plaintiffs have not alleged an archetypal fiduciary relationship with LastPass. So, the Court considers (1) "the relation of the parties," (2) "the plaintiff's business capacity contrasted with that of the defendant," (3) "the readiness of the plaintiff to follow the defendant's guidance in complicated transactions wherein the defendant has specialized knowledge," and (4) "the defendant's knowledge of the plaintiff's reliance." Id. (quoting Broomfield v. Kosow, 212 N.E.2d 556, 560 (Mass. 1965)).

Plaintiffs have not plausibly alleged a fiduciary relationship with LastPass. Plaintiffs claim they relied on LastPass's purported cybersecurity expertise and its promises to keep their data safe. But a "disparity of knowledge" is not enough to form a fiduciary relationship. See Geo. Knight & Co. v. Watson Wyatt & Co., 170 F.3d 210, 216 (1st Cir. 1999) (noting that "in most engagements of professional services," there is "a disparity of knowledge"). Nor is one party's trust that the other will perform its contractual obligations. Cf. Indus. Gen. Corp., 44 F.3d at 44 ("[T]he plaintiff alone, by reposing trust and confidence in the defendant, cannot thereby transform a business relationship into one which is fiduciary in nature." (quoting Superior Glass Co. v. First Bristol Cnty. Nat'l Bank, 406 N.E.2d 672, 674 (Mass. 1980))).

Rather, fiduciary relationships form when one party relies on the other's guidance and judgment in conducting complex transactions. See, e.g., Hawkes v. Lackey, 93 N.E. 828, 829 (Mass. 1911) (finding fiduciary relationship where defendant "ma[de] some investments for" plaintiffs with their money, and plaintiffs "apparently always did what he asked or advised" in financial matters); Reed v. A.E. Little Co., 152 N.E. 918, 920-21 (Mass. 1926) (finding fiduciary relationship where defendant company "undertook to be the plaintiff's adviser in the plaintiff's interest," and induced him to assign it rights to a valuable patent that it knew it could sell); Pearce v. Duchesneau Grp., Inc., 392 F. Supp. 2d 63, 70 (D. Mass. 2005) (considering how much discretion stockbroker had to trade on plaintiff's behalf when determining whether fiduciary relationship existed). Plaintiffs do not allege they relied on LastPass's guidance or business judgment, only on its assurances about the quality of its product. But that does not suffice. See Gemini Invs., Inc. v. Ches-Mont Disposal, LLC, 629 F. Supp. 2d 163, 169 (D. Mass. 2009) (holding that the defendant's "sales pitch with respect to its superior 'skill sets'" was "corporate puffery" that did not give rise to a fiduciary relationship). Thus, the motion to dismiss is **ALLOWED** as to the fiduciary duty claim (Count V).

8. Breach of Covenant of Good Faith and Fair Dealing (Count VI)

Next, Plaintiffs allege LastPass breached the implied covenant of good faith and fair dealing by providing inadequate cybersecurity, failing to timely and adequately notify Plaintiffs, and continuing to collect subscription fees after it discovered the breach. All contracts are "subject to an implied covenant of good faith and fair dealing." Robert & Ardis James Found. v. Meyers, 48 N.E.3d 442, 449 (Mass. 2016). It provides that "neither party shall do anything which will have the effect of destroying or injuring the right of the other party to receive the fruits of the contract." Druker v. Roland Wm. Jutras Assocs., Inc., 348 N.E.2d 763, 765 (Mass. 1976) (quoting Uproar Co. v. Nat'l Broad. Co., 81 F.2d 373, 377 (1st Cir. 1936)). To state a claim, the plaintiff must show the defendant "violate[d] [its] reasonable expectations," Chokel v. Genzyme Corp., 867 N.E.2d 325, 329 (Mass. 2007), and performed with a "lack of good faith," T.W. Nickerson, Inc. v. Fleet Nat'l Bank, 924 N.E.2d 696, 704 (Mass. 2010).

Plaintiffs have alleged LastPass acted with a "lack of good faith" by waiting four months to provide fulsome notice of the data breach. See Dkt. 86 at 61; see also Zoll Med. Corp. v. Barracuda Networks, Inc., 585 F. Supp. 3d 128, 138 (D. Mass. 2022). Thus, the motion to dismiss is **DENIED** as to Plaintiffs' good-faith-and-fair-dealing claim (Count VI).

9. Unjust Enrichment (Count VII)

Plaintiffs claim LastPass unjustly enriched itself by "fail[ing] to disclose facts pertaining to [its] substandard information systems," thereby "den[ying] Plaintiffs and Class Members the ability to make a rational and informed purchasing decision." See Dkt. 86 at 109. "[U]njust enrichment is defined as retention of money or property of another against the fundamental principles of justice or equity and good conscience." Doe v. Tenet Healthcare Corp., No. 23-12978, 2024 WL 1756075, at *5 (D. Mass. Apr. 23, 2024) (cleaned up) (quoting Sacks v. Dissinger, 178 N.E.3d 388, 397 (Mass. 2021)). LastPass argues Plaintiffs have "adequate remed[ies] at law" so they cannot recover for unjust enrichment. See Dkt. 92-1 at 39 (quoting Fernandez v. Havkin, 731 F. Supp. 2d 103, 114 (D. Mass. 2010)).

A "party with an adequate remedy at law cannot claim unjust enrichment." Tomasella v. Nestlé USA, Inc., 962 F.3d 60, 82 (1st Cir. 2020) (quoting Shaulis v. Nordstrom, Inc., 865 F.3d 1, 16 (1st Cir. 2017)). The inquiry turns on "the availability of a remedy at law, not the viability of that remedy." Id. at 82-83 (emphasis added) (quoting Shaulis, 865 F.3d at 16). Here, Plaintiffs have adequate remedies available at law, for example, through their Massachusetts Consumer Protection Act and breach of contract claims. See id. at 84 (holding that the plaintiff's "unjust enrichment claims must be dismissed because an adequate

remedy at law was undoubtedly available to her through Chapter 93A"). Thus, the motion to dismiss Plaintiffs' unjust enrichment claim (Count VII) is **ALLOWED**.

10. Declaratory and Injunctive Relief (Count VIII)

Plaintiffs seek a declaratory judgment that LastPass breached duties owed to customers and an injunction requiring LastPass to improve its security protocols. See Dkt. 86 at 111.[13] The Declaratory Judgment Act grants courts discretion to "declare the rights and other legal relations of any interested party . . . but only in [] case[s] of actual controvers[ies] within that court's jurisdiction." In re Fin. Oversight & Mgmt. Bd. For P.R., 916 F.3d 98, 110 (1st Cir. 2019) (cleaned up) (quoting 28 U.S.C. § 2201(a)). Given "the nonobligatory nature of the remedy, a district court is authorized, in the sound exercise of its discretion, to stay or to dismiss an action seeking a declaratory judgment before trial." Wilton v. Seven Falls Co., 515 U.S. 277, 288 (1995). The Court does not entertain the request for a declaratory judgment in light

[13] Although Plaintiffs invoke the Court's authority to issue declaratory judgments pursuant to the "Massachusetts Declaratory Judgment Act [and] the Federal Rules of Civil Procedure," Dkt. 86 at 111, the Court considers this count under the federal Declaratory Judgment Act, see Tocci Bldg. Corp. of N.J., Inc. v. Va. Sur. Co., 750 F. Supp. 2d 316, 320 n.2 (D. Mass. 2010) ("A declaratory judgment action is procedural only. . . . [and] is properly considered under the federal Declaratory Judgment Act rather than under Massachusetts' Declaratory Judgment Act." (internal citations omitted)).

of the many viable state law claims. LastPass's motion to dismiss is **ALLOWED** as to the request for declaratory relief (Count VIII).

11. State Statutory Claims

Plaintiffs bring a plethora of claims under the Massachusetts Consumer Protection Act and twelve other state statutes. LastPass moves to dismiss on various grounds. These claims are sparsely briefed by both sides.

a. Extraterritoriality (Counts XI, XIX, XX & XXI)

LastPass argues Plaintiffs impermissibly seek to apply the Arizona Consumer Fraud Act ("ACFA"), Illinois Deceptive Trade Practices Act ("IDTPA"), New York General Business Law ("NYGBL"), and Oklahoma Consumer Protection Act ("OCPA") extraterritorially. The ACFA, IDTPA, NYGBL, and OCPA cover only those transactions that occurred in their respective states. See Thuney v. Lawyer's Title of Ariz., No. 18-1513, 2019 WL 467653, at *6 (D. Ariz. Feb. 6, 2019) (quoting State ex rel. Corbin v. Goodrich, 726 P.2d 215, 221 (Ariz. Ct. App. 1986) (ACFA); IPOX Schuster, LLC v. Nikko Asset Mgmt. Co., 191 F. Supp. 3d 790, 807-08 (N.D. Ill. 2016) (IDTPA); Goshen v. Mut. Life Ins. Co. of N.Y., 774 N.E.2d 1190, 1195-96 (N.Y. 2002) (NYGBL); Steinbeck v. Dollar Thrifty Auto. Grp., Inc., No. 08-0378, 2008 WL 4279798, at *3 (N.D. Okla. Sept. 15, 2008) (citing Harvell v. Goodyear Tire & Rubber Co., 164 P.3d 1028, 1037 (Okla. 2006)) (OCPA). Some courts use multifactor tests to determine whether a transaction has occurred within the state.

See, e.g., IPOX Schuster, 191 F. Supp. 3d at 808 ("Courts weigh four factors in determining whether a transaction occurred primarily and substantially in Illinois: (1) the plaintiff's residence, (2) where the misrepresentation was made, (3) where the damage to the plaintiff occurred, and (4) whether the plaintiff communicated with the defendant in Illinois." (cleaned up) (quoting Specht v. Google, Inc., 660 F. Supp. 2d 858, 866 (N.D. Ill. 2009))). The parties have done a poor job briefing the standards in each of these states for determining whether the statute applies. Moreover, Plaintiffs have not pleaded sufficient facts to show they transacted in the states at issue. Mere residence at the time of filing the complaint is insufficient. So, the motion to dismiss is **ALLOWED** as to Counts XI, XIX, XX & XXI.

b. Rule 9(b) (Counts XII, XIII & XVI)

LastPass argues Plaintiffs' claims under the California Unfair Competition Law ("CUCL"), California Consumer Legal Remedies Act ("CCLRA"), and Florida Deceptive and Unfair Trade Practices Act ("FDUTPA") fail to meet Rule 9(b)'s heightened pleading standards. Rule 9(b) requires that a plaintiff bringing a claim that sounds in fraud "must state with particularity the circumstances constituting fraud or mistake." Fed. R. Civ. P. 9(b). LastPass contends Plaintiffs' claims under these statutes sound in fraud, so Rule 9(b) applies. See Univ. Commc'n Sys., Inc. v. Lycos, Inc., 478 F.3d 413, 427 (1st. Cir. 2007) (holding Rule 9(b) applies

to state fraud claims brought in federal court); In re Sony Gaming Networks & Customer Data Sec. Breach Litig., 996 F. Supp. 2d 942, 989 (applying Rule 9(b) to fraudulent misrepresentation claims under CUCL and CCLRA); State Farm Mut. Auto. Ins. Co. v. Performance Orthopaedics & Neurosurgery, LLC, 278 F. Supp. 3d 1307, 1328 (S.D. Fla. 2017) (holding that "where the gravamen of the [FDUTPA] claim sounds in fraud, . . . Rule 9(b) applies" (citations omitted)). Plaintiffs disagree, stating that as a legal matter, they are not required to plead specific misrepresentations under these statutes. But Plaintiffs cite no relevant caselaw. The motion to dismiss Counts XII, XIII & XVI is **ALLOWED** to the extent Plaintiffs' claims are based on LastPass's allegedly fraudulent misrepresentations. But the motion is **DENIED** to the extent the claims are based on LastPass's allegedly negligent misrepresentations or unfair acts or practices, like failure to maintain reasonable security measures.

c. Sufficiency of Allegations (Counts IX, X & XII)

LastPass argues that Plaintiffs' claims under Chapter 93A and the California Unfair Competition Law ("CUCL") are "conclusory" because Plaintiffs do not "sufficiently plead misrepresentations which caused their alleged injuries." Dkt. 92-1 at 41 (emphasis omitted). But both Chapter 93A and the CUCL prohibit unfair trade practices, not just deceptive ones. See Aliberti, 133 N.E.3d at

291; Kwikset Corp. v. Superior Ct., 246 P.3d 877, 885 (Cal. 2011). Plaintiffs allege a variety of unfair practices, including that LastPass "fail[ed] to comply with common law and statutory duties," and that LastPass employed unreasonably weak internal and external cybersecurity protocols. See Dkt. 86 at 113-14, 119-20. The Court declines to dismiss these counts on sufficiency grounds. The motion to dismiss is **DENIED** on this ground as to Counts IX, X & XII.

d. Application of the California Customer Records Act and California Consumer Privacy Act (Counts XIV & XV)

LastPass argues the California Customer Records Act ("CCRA") and the California Consumer Privacy Act ("CCPA") do not apply because Plaintiffs' "sensitive data remained encrypted." Dkt. 92-1 at 43, 45. Both statutes define "[p]ersonal information" as "[a]n individual's first [and] last name in combination with" enumerated "data elements, when either the name or the data elements are not encrypted or redacted." See Cal. Civ. Code § 1798.81.5(d)(1)(A) (emphasis added); id. § 1798.150(a)(1). Data elements listed include social security numbers, credit or debit card numbers with an access code, and medical information, health insurance information, and biometric data. Id. § 1798.81.5(d)(1)(A)(i)-(vi). Here, Plaintiffs allege the breach resulted in exfiltration of their unencrypted names along with encrypted vault data including credit card numbers, social security numbers, and more.

Plaintiffs' exfiltrated data fits the statutory definition. The motion to dismiss is **DENIED** on this ground as to Count XIV.

As to the CCPA claim, LastPass also argues Plaintiffs have only "suggest[ed] that LastPass failed to follow appropriate cybersecurity practices," which is insufficient. See Dkt. 92-1 at 45. But LastPass misapprehends the consolidated complaint, which alleges, among other things, that LastPass's password encryption algorithm fell below industry standards. Plaintiffs have plausibly alleged LastPass violated "the duty to implement and maintain reasonable security procedures." Cal. Civ. Code § 1798.150(a)(1). The motion to dismiss Count XV on this ground is **DENIED**.

e. Pre-Suit Notice (Counts XIII & XV)

LastPass also argues Plaintiffs failed to satisfy the pre-suit notice requirements of the California Consumer Legal Remedies Act ("CCLRA") and California Consumer Privacy Act ("CCPA"). Under the CCLRA, a plaintiff seeking damages must provide notice at least thirty days prior to initiating suit. See Cal. Civ. Code § 1782(b). Likewise, the CCPA requires plaintiffs seeking statutory damages to provide a defendant "30 days' written notice identifying the specific provisions of [the CCPA] the consumer alleges have been or are being violated." Id. § 1798.150(b). The parties have not cited relevant caselaw construing CCPA's pre-suit notice requirement. But in suits under the CCLRA, some courts have held that notice sent thirty days prior to the operative complaint

suffices. See Corra v. Energizer Holdings, Inc., 962 F. Supp. 2d 1207, 1220-21 (E.D. Cal. 2013) (holding that because notice letters preceded first amended complaint "by more than thirty days, Plaintiff was entitled to request damages" in the first amended complaint "regardless of whether she could have done so in the [initial] complaint"); Shein v. Canon U.S.A., Inc., No. 08-07323, 2009 WL 3109721, at *6 (C.D. Cal. Sept. 22, 2009) (holding that because plaintiffs sent demand letter over thirty days before filing the third amended complaint, it "constitute[d] timely CLRA notice" even though the suit was filed over a year prior).

This case started on December 2, 2022, when Debt Cleanse filed a class action complaint against Defendants. See Dkt. 1. Debt Cleanse, a Delaware LLC operating in Illinois, did not raise a CCPA claim. After moving to consolidate several cases stemming from the data breach, Plaintiffs sent Defendants CCPA notice letters on January 16 and February 21, 2023. After the Court consolidated the cases, on August 4, 2023, Plaintiffs filed the operative consolidated complaint. See Dkt. 86. It was the first pleading to name Californian plaintiffs and CCPA claims.

Plaintiffs' January 16 and February 21 notices were timely. The motion to dismiss is **DENIED** on this ground as to the CCLRA and CCPA (Counts XIII & XV).[14]

[14] The CCPA does not require pre-suit notice for plaintiffs who seek compensatory damages as opposed to statutory damages. See

f. Applicability of the Pennsylvania Unfair Trade Practices and Consumer Protection Law (Count XXII)

LastPass argues Plaintiffs have not stated a claim under the Pennsylvania Unfair Trade Practices and Consumer Protection Law ("PUTPCPL") because no Plaintiff lives in Pennsylvania and the only one who resided there did not pay for LastPass. The PUTPCPL authorizes suit by "[a]ny person who purchases or leases goods or services primarily for personal, family[,] or household purposes" and is injured as a result. See 73 Pa. Cons. Stat. § 201-9.2(a). Plaintiffs do not respond to LastPass's argument. Thus, the motion to dismiss Count XXII is **ALLOWED** as unopposed.

g. Illinois Personal Information Protection Act and Illinois Consumer Fraud and Deceptive Business Practices Act (Counts XVII & XVIII)

Beyond their arguments on standing and actual loss, Defendants do not challenge the claims under the Illinois Personal Information Protection Act (Count XVII) and the Illinois Consumer Fraud and Deceptive Business Practices Act (Count XVIII). Because Plaintiffs have plausibly shown they have standing and have alleged a cognizable injury as described above, the motion to dismiss is **DENIED** as to Counts XVII and XVIII.

Cal. Civ. Code § 1798.150(b). Two of the three Californian Plaintiffs suffered pecuniary losses due to the breach. Inadequate pre-suit notice would not be fatal to their claims.

ORDER

For the reasons stated above, Defendants' motion to dismiss (Dkt. 92) is **ALLOWED** as to all claims against GoTo. The motion to dismiss is **ALLOWED** as to Plaintiffs' claims against LastPass for negligence (Count I), breach of implied contract (Count IV), breach of fiduciary duty (Count V), unjust enrichment (Count VII), declaratory relief (Count VIII), and violations of the Arizona Consumer Fraud Act (Count XI), Illinois Deceptive Trade Practices Act (Count XIX), New York General Business Law (Count XX), Oklahoma Consumer Protection Act (Count XXI), and Pennsylvania Unfair Trade Practices and Consumer Protection Law (Count XXII). The motion to dismiss is **DENIED** as to Plaintiffs' claims against LastPass, for breach of contract (Count III), breach of the covenant of good faith and fair dealing (Count VI), and violations of Chapter 93A (Counts IX & X), California Customer Records Act (Count XIV), California Consumer Privacy Act (Count XV), Illinois Personal Information Protection Act (Count XVII), and Illinois Consumer Fraud and Deceptive Business Practices Act (Count XVIII). With respect to Plaintiffs' claim against LastPass for negligent misrepresentation (Count II), the motion to dismiss is **DENIED** as to Debt Cleanse but **ALLOWED** as to other Plaintiffs. With respect to Plaintiffs' claims against LastPass under the California Unfair Competition Law (Count XII), California Consumer Legal Remedies Act (Count XIII), and Florida Deceptive and Unfair Trade Practices

Act (Count XVI), the motion to dismiss is **ALLOWED** as to allegations of fraudulent misrepresentations, but otherwise is **DENIED**.

SO ORDERED.

/s/ PATTI B. SARIS
Hon. Patti B. Saris
United States District Judge